



NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

[NOTICE: 23-048]

Privacy Act of 1974; System of Records

AGENCY: Office of the Inspector General (OIG), National Aeronautics and Space Administration (NASA).

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the National Aeronautics and Space Administration (NASA) is issuing public notice of modification to a previously announced system of records, The Office of Inspector General Advanced Data Analytics System (ADAS), NASA 10IGDA. This notice incorporates locations and NASA standard routine uses previously published separately from, and cited by reference in, this and other NASA systems of records notices. This notice also updates individual and record categories, technical safeguards and revises routine uses. The system of records is more fully described in the **SUPPLEMENTARY INFORMATION** section of this notice.

DATES: NASA seeks comment on the revised system of records described in this notice, in accordance with the requirements of the Privacy Act. We must receive your comments about the new system of records within 30 calendar days from the date of this publication. The changes will take effect at the end of that period if no adverse comments are received.

ADDRESSES: Bill Edwards-Bodmer, Privacy Act Officer, Office of the Chief Information Officer, National Aeronautics and Space Administration Headquarters, Washington, DC 20546-0001, (757) 864-7998, NASA-PAOfficer@nasa.gov.

FOR FURTHER INFORMATION CONTACT: NASA Privacy Act Officer, Bill Edwards-Bodmer, (757) 864-7998, NASA-PAOfficer@nasa.gov.

SUPPLEMENTARY INFORMATION: This system notice includes minor revisions to NASA's existing system of records notice, to bring its format into compliance with OMB

guidance, and to update records access, notification, and contesting procedures consistent with NASA Privacy Act regulations. It incorporates in whole information formerly published separately in the *Federal Register* as appendix A, Location Numbers and Mailing Addresses of NASA Installations at which Records are Located, and appendix B, Standard Routine Uses – NASA, and removes references to appendix A and appendix B. The notice updates the **ROUTINE USES** section to conform to provisions of the Inspector General Empowerment Act of 2016, which exempted Inspectors General from requirements of the Computer Matching and Privacy Protection Act of 1988, when conducting an audit, investigation, inspection, evaluation, or other review authorized under the Inspector General Act of 1978, as amended, 5 U.S.C. 401 et seq. This notice updates **CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM, CATEGORIES OF RECORDS IN THE SYSTEM, and RECORD SOURCE CATEGORIES** to reflect current information for those categories. Finally, this notice updates **PHYSICAL SAFEGUARDS** to reflect current information technology security protocols.

William Edwards-Bodmer,

NASA Privacy Act Officer.

SYSTEM NAME AND NUMBER: Office of the Inspector General Advanced Data Analytics System (ADAS),NASA 10IGDA.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Electronic records are migrating from a secure NASA server to a secure cloud maintained by Amazon Web Services (AWS), 410 Terry Ave., North Seattle, WA 98109.

Paper records are maintained at the Office of Inspector General, Advanced Data Analytics Program (ADAP), Mary W. Jackson NASA Headquarters, National Aeronautics and Space Administration (NASA), 300 E Street SW, Suite 8W37, Washington, DC 20546, and other OIG field locations.

SYSTEM MANAGER(S): OIG Chief Data Officer, NASA Office of Inspector General, 300 E Street SW, Suite 8W37, Washington, DC 20546-0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 404 (a).

PURPOSE(S) OF THE SYSTEM: This system of records is maintained for the general purpose of enabling OIG to fulfill the requirements of section 404, para. (a)(1) and (3), of the Inspector General Act of 1978, as amended, 5 U.S.C. 401 et seq., which requires OIG to provide policy direction for and to conduct, supervise, and coordinate audits and investigations relating to the programs and operations of NASA and to conduct, supervise and coordinate activities for the purpose of promoting economy and efficiency in the administration of, or preventing and detecting fraud and abuse in, the programs and operations of NASA. This system is maintained for the purpose of improving the efficiency, quality, and accuracy of existing data collected by NASA. Records in this system will be used to conduct data modeling for indications of fraud, abuse and internal control weaknesses concerning NASA programs and operations. The result of that data modeling may be used in the conduct of audits, investigations, inspections, or other activities as necessary to prevent and detect waste, fraud, and abuse and to promote economy and efficiency in NASA programs and operations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: This system maintains information on (1) current and former employees of NASA; (2) current and former NASA contractors and subcontractors; (3) current and former NASA grantees and subgrantees; (4) and other persons whose actions may have affected NASA or may have affected individuals listed in (1) through (3) above.

CATEGORIES OF RECORDS IN THE SYSTEM: Data sets pertaining to matters including, but not limited to, the following (1) fraud against the Government; (2) theft of Government property; (3) bribery; (4) misuse of funds; (5) misuse of Government property; (6) conflict of interest; (7) waiver of claim for overpayment of pay; (8) unauthorized disclosure of Source Evaluation Board information; (9) improper personal conduct; (10) irregularities in the procurement process, including but not limited to, contracts, grants, subcontracts, and subgrants; (11) computer crimes; (12) research misconduct; and (13) data relating to statutes and regulations that affect NASA, NASA employees, NASA property, NASA contractors/grantees, and NASA subcontractor/subgrantees. Specific record fields may include, but are not limited to, information such as: name, social security number, date of birth, phone numbers, addresses, pay/leave information, and other data available in systems described in **RECORD SOURCE CATEGORIES**.

RECORD SOURCE CATEGORIES: This system contains records taken from, but not limited to, the following NASA systems: Core Financial Management Records (System Number 10CFMR) , NASA Education Program Evaluation System (System Number 10EDUA, NASA Guest Operations System (System Number 10GOS), Inspector General Investigations Case Files (System Number 10IGIC), NASA Personnel and Payroll Systems (System Number 10NPPS), Parking and Transit System (System Number 10PATs), Security Records System (System Number 10SECR), Special Personnel Records (System Number 10SPER), Exchange Records on Individuals (System Number 10XROI), as well as data obtained as a result of cooperation efforts

between OIGs, the Council of the Inspectors General on Integrity and Efficiency, and the Pandemic Response Accountability Committee.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING

CATEGORIES OF USERS AND PURPOSES FOR SUCH USES: The NASA OIG may disclose information contained in a record in this system of records without the consent of the individual if the disclosure is compatible with the purpose for which the record was collected, under the following routine uses.

The NASA OIG may make these disclosures on a case-by-case basis, or as part of computerized data comparisons of Federal systems of records, or of a Federal system of records with other records (including non-Federal records) performed in connection with an audit, investigation, inspection, evaluation, or other review authorized under the IG Act and IG Empowerment Act of 2016. Under the following routine uses that are unique to this system of records, information in this system may be disclosed when:

1. Responding to inquiries from the White House, the Office of Management and Budget, and other organizations in the Executive Office of the President.
2. Disclosing to a Federal, State, local, tribal, or territorial government or agency lawfully engaged in the collection of intelligence (including national intelligence, foreign intelligence, and counterintelligence), counterterrorism, or homeland security, law enforcement or law enforcement intelligence, and other information, where disclosure is undertaken for intelligence, counterterrorism, homeland security, or related law enforcement purposes, as authorized by U.S. Law or Executive Order, and in accordance with applicable disclosure policies.
3. Disclosing to any official (including members of the Council of Inspectors General on Integrity and Efficiency (CIGIE) and staff and authorized officials of the Department of Justice and Federal Bureau of Investigation) charged with the responsibility to conduct

qualitative assessment reviews of internal safeguards and management procedures employed in Office of Inspector General (OIG) operations.

4. Disclosing to members of the CIGIE for the preparation of reports to the President and Congress on the activities of the Inspectors General.

In addition, information may be disclosed under the following NASA Standard Routine Uses wherein references to NASA shall be deemed to include NASA OIG:

1. Law Enforcement — When a record on its face, or in conjunction with other information, indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order, disclosure may be made to the appropriate agency, whether Federal, foreign, State, local, or tribal, or other public authority responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order, if NASA determines by careful review that the records or information are both relevant and necessary to any enforcement, regulatory, investigative or prosecutive responsibility of the receiving entity.
2. Certain Disclosures to Other Agencies — A record from this SOR may be disclosed to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary, to obtain information relevant to a NASA decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.
3. Certain Disclosures to Other Federal Agencies — A record from this SOR may be disclosed to a Federal agency, in response to its request, for a matter concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license,

grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

4. Department of Justice — A record from this SOR may be disclosed to the Department of Justice when a) NASA, or any component thereof; or b) any employee of NASA in his or her official capacity; or c) any employee of NASA in his or her individual capacity where the Department of Justice has agreed to represent the employee; or d) the United States, where NASA determines that litigation is likely to affect NASA or any of its components, is a party to litigation or has an interest in such litigation, and by careful review, the use of such records by the Department of Justice is deemed by NASA to be relevant and necessary to the litigation.
5. Courts — A record from this SOR may be disclosed in an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when NASA determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant and necessary to the proceeding.
6. Response to an Actual or Suspected Compromise or Breach of Personally Identifiable Information — A record from this SOR may be disclosed to appropriate agencies, entities, and persons when (1) NASA suspects or has confirmed that there has been a breach of the system of records; (2) NASA has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, NASA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with NASA's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
7. Contractors — A record from this SOR may be disclosed to contractors, grantees, experts, consultants, students, volunteers, and others performing or working on a

contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish a NASA function related to the SOR.

Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to NASA employees.

8. Members of Congress — A record from this SOR may be disclosed to a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.
9. Disclosures to Other Federal Agencies in Response to an Actual or Suspected Compromise or Breach of Personally Identifiable Information — A record from this SOR may be disclosed to another Federal agency or Federal entity, when NASA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.
10. National Archives and Records Administration — A record from this SOR may be disclosed as a routine use to the officers and employees of the National Archives and Records Administration (NARA) pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.
11. Audit — A record from this SOR may be disclosed to another agency, or organization for purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records in this system are maintained as hard-copy documents and on electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records in this system of records are retrieved by name or other identifying information of an individual or institution.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are maintained in Agency files and destroyed in accordance with NASA Procedural Requirements (NPR) 1441.1, NASA Records Retention Schedules, Schedule 9. Files containing information of an investigative nature but not related to a specific investigation are destroyed in accordance with NPR 1441.1.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Electronic records are maintained on a secure NASA server until migration to a secure cloud maintained by AWS.

Paper and electronic records are protected in accordance with all Federal standards and those established in NASA regulations at 14 CFR 1212.605. Additionally, server and data management environments employ infrastructure encryption technologies both in data transmission and at rest on servers. Electronic messages sent within and outside of the Agency that convey sensitive data are encrypted and transmitted by staff via pre-approved electronic encryption systems as required by NASA policy. Approved security plans are in place for information systems containing the records in accordance with the Federal Information Security Management Act of 2002 (FISMA) and OMB Circular A-130, Management of Federal Information Resources. Only authorized personnel requiring information in the official discharge of their duties are authorized access to records through approved access or authentication methods. Access to electronic records is achieved only from workstations within the NASA Intranet, or remotely via a secure Virtual Private Network (VPN) connection requiring two-factor token authentication or via employee PIV badge authentication from NASA-issued computers. Non-electronic records are secured in locked rooms or files.

RECORD ACCESS PROCEDURES: In accordance with 14 CFR part 1212, Privacy Act – NASA Regulations, information may be obtained by contacting in person or in writing the system or subsystem manager listed above at the location where the records are created and/or

maintained. Requests must contain the identifying data concerning the requester, e.g., first, middle and last name; date of birth; description and time periods of the records desired. NASA Regulations also address contesting contents and appealing initial determinations regarding records access.

CONTESTING RECORD PROCEDURES: In accordance with 14 CFR part 1212, Privacy Act – NASA Regulations, information may be obtained by contacting in person or in writing the system or subsystem manager listed above at the location where the records are created and/or maintained. Requests must contain the identifying data concerning the requester, e.g., first, middle and last name; date of birth; description and time periods of the records desired. NASA Regulations also address contesting contents and appealing initial determinations regarding records access.

NOTIFICATION PROCEDURES: In accordance with 14 CFR part 1212, Privacy Act – NASA Regulations, information may be obtained by contacting in person or in writing the system or subsystem manager listed above at the location where the records are created and/or maintained. Requests must contain the identifying data concerning the requester, e.g., first, middle and last name; date of birth; description and time periods of the records desired. NASA Regulations also address contesting contents and appealing initial determinations regarding records access.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: As described above, the ADAS will consist primarily of records compiled from existing systems of records maintained by NASA and other Federal agencies. The OIG will continue to apply to individual records within the ADAS any Privacy Act exemptions which apply to the system(s) from which the relevant record(s) originated. The Privacy Act Systems of Records Notices which describe in detail the exemptions claimed for each NASA system from which ADAS records will be derived can be found online at the following web address: http://www.nasa.gov/privacy/nasa_sorn_index.html.

HISTORY: (15-108, 80 FR 72745, pp. 72745-72750).

[FR Doc. 2023-09935 Filed: 5/9/2023 8:45 am; Publication Date: 5/10/2023]